REMARKS

Claims 1, 5, 6, 7, and 9-28 are pending in this application. Claims 1, 5, 6, 7, 9-14, and 16-26 are amended herein. Claims 2, 3, 4, and 8 are cancelled herein without prejudice or disclaimer. Support for the amendments to the claims may be found in the claims as originally filed. Reconsideration is requested based on the foregoing amendment and the following remarks.

Response to Arguments:

The Applicants appreciate the consideration given to their arguments. Further favorable consideration is requested.

Objection to the Title of the Invention:

The Title of the Invention was objected to as not descriptive. The Title has been replaced with a new Title in substantial accord with the Examiner's suggestion. The Examiner's suggestion is appreciated. Withdrawal of the objection is earnestly solicited.

Objections to the Specification:

The Specification was objected to for failing to provide proper antecedent basis for the claimed subject matter. The Office Action asserts in section 8, at page 7, that:

> The specification discloses that predetermined information is encrypted to produce license information.

This is submitted to be incorrect. As described in the specification, rather, at page 4, line 25, continuing at page 5, lines 1 and 2, "the predetermined information stored in the first area *includes* license information based on use rights for using the electronic data," with emphasis added. Thus, it is submitted to be entirely proper that, as also noted astutely in the Office Action in section 8, at page 7:

> The claims recite "predetermined information" and "license information", however the specification does not disclose both data being separate data.

Still, in the interest of compact prosecution only, and not for any reason of patentability, claim 1, for example, has been amended to recite "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information." The Specification is thus submitted to provide proper antecedent basis for the claimed subject matter. Withdrawal of the objection is

earnestly solicited.

Claim Rejections - 35 U.S.C. § 112:

Claims 6, 7, 9, 10, 16, 18-26 and 28 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. The rejection is traversed. The Office Action asserts in section 5, at page 2, that:

> The specification discloses that predetermined information is encrypted to produce license information.

This is submitted to be incorrect. As described in the specification, rather, at page 4, line 25, continuing at page 5, lines 1 and 2, "the predetermined information stored in the first area includes license information based on use rights for using the electronic data." Thus, it is submitted to be entirely proper that, as also noted astutely in the Office Action in section 5, at page 2:

> The claims recite "predetermined information" and "license information", however the specification does not disclose both data being separate data.

Still, in the interest of compact prosecution only, and not for any reason of patentability, claim 18, for example, has been amended to recite "predetermined information deriving means encrypting said license information stored in said secure area using said medium-specific information or a key generated therefrom." Claims 6, 7, 9, 10, 16, 18-26, and 28 are thus submitted to comply with the written description requirement of 35 U.S.C. § 112, first paragraph. Withdrawal of the rejection is earnestly solicited.

35 U.S.C. § 112, second paragraph:

Claims 1, 6, and 9-28 were rejected under 35 U.S.C. § 112, second paragraph, as indefinite. Claims 1, 5, 6, 7, 9-14, and 16-26 were amended to make them more definite. The Examiner's suggestions are appreciated. Withdrawal of the rejection is earnestly solicited.

Claim Rejections - 35 U.S.C. § 102:

Claims 1, 11, and 27 were rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent No. 5,905,798 to Nerlikar et al. (hereinafter "Nerlikar"). The rejection is traversed to the extent it would apply to the claims as amended. Reconsideration is earnestly solicited.

The third clause of claim 1 recites:

> Storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as

the predetermined information.

Nerlikar neither teaches, discloses, nor suggests "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," as recited in claim 1. In Nerlikar, rather, if the codeword and/or the predetermined address are encrypted by the transponder, then the interrogator *decrypts* the codeword and/or the predetermined address, not stores them. In particular, as described at column 3, lines 22-28:

> The final 32 bits, shown for illustrative purposes only, may comprise a 32 bit code used in a decryption scheme if applicable, i.e. if the codeword and/or the predetermined address are encrypted by the transponder, the transponder may send an up to 32 bit decryption scheme with the encrypted codeword and/or predetermined address with which to allow the interrogator to decrypt.

Since, in Nerlikar, the interrogator decrypts the codeword and/or the predetermined address if the transponder encrypted them, Nerlikar is not "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," as recited in claim 1.

Nerlikar, furthermore, never *stores* encrypted information outside the transponder, to which the Office Action analogizes the "predetermined secure area" of the claimed invention, at all. In Nerlikar, rather, the codeword or the predetermined address may be encrypted within the transponder according to some predetermined algorithm. In particular, as described at column 2, lines 36-39:

> In other words, both or either the codeword or the predetermined address may be encrypted within the transponder according to some predetermined algorithm preprogrammed at the manufacturing level or programmed by the customer. In the case of an encrypted codeword and address, both would then be decrypted by the interrogation section of the media player upon receipt of such.

Since, in Nerlikar, the codeword or the predetermined address may be encrypted within the transponder according to some predetermined algorithm, Nerlikar is not "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," as recited in claim 1.

The fourth clause of claim 1 recites:

> Deriving the license information outside said secure area of the recording medium.

Nerlikar neither teaches, discloses, nor suggests "deriving the license information outside said

secure area of the recording medium," as recited in claim 1. In Nerlikar, rather, the interrogator decrypts the codeword and/or the predetermined address upon receipt, not stores them, as discussed above. Since the interrogator decrypts the codeword and/or the predetermined address, rather than storing them, there is no "license information outside said secure area of the recording medium" in Nerlikar to derive. Claim 1 is submitted to be allowable. Withdrawal of the rejection of claim 1 is earnestly solicited.

Claims 11 and 27 depend from claim 1 and add further distinguishing elements. Claims 11 and 27 are thus also submitted to be allowable. Withdrawal of the rejection of claims 11 and 27 is also earnestly solicited.

Claims 1, 6, 11, 18, 27, and 28:

Claims 1, 6, 11, 18, 27, and 28 were rejected under 35 U.S.C. § 102(e) as anticipated by U.S. Patent Application Publication No. 2002/0016919 to Sims, III (hereinafter "Sims"). The rejection is traversed to the extent it would apply to the claims as amended. Reconsideration is earnestly solicited.

Sims neither teaches, discloses, nor suggests "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," as recited in claim 1. In Sims, rather, the encrypted disk key is *provided* to the play-back device decoder at step 313 to allow meaningful use of the content recorded thereon, not stored. The encrypted disk key, in particular, must needs be decrypted in order to allow meaningful use of the content recorded thereon. In particular, as described at paragraph [0097]:

> At step 310 the requested "acceptable user" is validated against the list of "acceptable users" and, provided it is indeed a match, the disk key, here the content key, is read from the media (step 311) and encrypted with the public key of the matching "acceptable user" (step 312). Thereafter this encrypted disk key is provided to the play-back device decoder at step 313 to allow meaningful use of the content recorded thereon and operation according to the present invention is concluded. It shall be appreciated that, as the disk key is encrypted utilizing the public key of the particular decoder, that only this device may actually decrypt the content of media 100 even if a rogue were to emulate the above preceding steps.

Since, in Sims, the encrypted disk key is provided to the play-back device decoder at step 313 to allow meaningful use of the content recorded thereon, Sims is not "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," as recited in claim 1.

Sims, furthermore, only stores encrypted *content* in unsecured area 102 of media 100.

In particular, as described at paragraph [0086]:

> At step 209 it is determined whether the particular implementation of the present invention includes the encrypting of content to be stored in unsecured area 102 of media 100. If no encryption of this content is desired, i.e. encryption is utilized for media authentication only, then operation proceeds to step 214 wherein the content is recorded to media 100.

Since Sims stores encrypted content in unsecured area 102 of media 100, Sims is not "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," as recited in claim 1.

Furthermore, in Sims, the private keys may not even be *revealed* to any party. In particular, as described at paragraph [0019]:

> Moreover, as these private keys may be embedded within circuitry useful in encrypting/decrypting information according to the present invention, the private keys may not even be revealed to any party.

Since, in Sims, the private keys may not even be revealed to any party, Sims is not "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," as recited in claim 1.

Furthermore, in Sims, the key is *securely* stored by the media which actively operates to securely transmit this key to the play-back device without *ever* disclosing the key to the media device. In particular, as described at paragraph [0020]:

> In an alternative embodiment, rather than storing the content key in an area of limited access on the media, for retrieval by the media device and subsequent transmission to the play-back device, the key is securely stored by the media which actively operates to securely transmit this key to the play-back device without ever disclosing the key to the media device. Accordingly, the active component utilized for hiding this key not in the media device or disk drive. Instead, it is a portion of the media, such as an electronic circuit including a processor and memory operating under control of an internal algorithm.

Since, in Sims, the key is securely stored by the media which actively operates to securely transmit this key to the play-back device without ever disclosing the key to the media device, Sims is not "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," as recited in claim 1.

Furthermore, in Sims, information such as cryptographic keys may be stored in *protected*

storage area 101 of media 100. In particular, as described at paragraph [0042]:

> In an alternative embodiment of the present invention protected storage area 101 is an active portion of media 100, such as may be provided by a processor and associated memory. Accordingly, information, such as cryptographic keys utilized according to the present invention may be stored therein and provided externally only upon select conditions.

Since, in Sims, information such as cryptographic keys may be stored in *protected* storage area 101 of media 100, Sims is not "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," as recited in claim 1.

Furthermore, in Sims, information that is to be protected, or provided limited access, may be disbursed throughout unprotected area 102 in a manner such that its recovery is *impossible* or *unlikely* except to devices operating according to the present invention. Sims, thus, converts the unprotected area of media 100 in which information is disbursed into a secured area inaccessible to the usual devices. In particular, as described at paragraph [0047]:

> In another alternative embodiment, protected area 101 is not a discrete portion of media 100, but rather is information provided in a secured fashion within the unprotected area of media 100. For example, information which is to be protected, or provided limited access, according to the present invention may be disbursed throughout unprotected area 102 in a manner such that its recovery is impossible or unlikely except to devices operating according to the present invention. Accordingly, in an embodiment of the present invention, information stored in protected area 101 is encoded as errors in the information stored in unprotected area 102. These errors are predetermined to be correctable, such as through CRC error correction algorithms known in the art, in order to provide error free utilization of the information stored in unprotected area 102. However, the placement of such errors and/or particular patterns of the errors are utilized to encode the information of protected area 101. Such an embodiment may be utilized to prevent unauthorized copying as a system providing anything other than a raw data copy will likely used the CRC algorithms to "correct" those errors prior to their being written on the copy.

Since, in Sims, information which is to be protected, or provided limited access, may be disbursed throughout unprotected area 102 in a manner such that its recovery is impossible or unlikely except to devices operating according to the present invention, Sims is not "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," as recited in claim 1.

Finally, in Sims, the media device honoring the technique of the present invention is allowed to pass the disk key to this content provider using this public key provided on the media.

The media device is then able to *decrypt* that list with this key. In particular, as described at paragraph [0095]:

> For example, the media device may establish communication with a clearing house and identify itself to the service provider, such as through the use of one of the acceptable keys on the list being that of the person who owns the content itself, i.e., the media public key. Accordingly, the media device honoring the technique of the present invention is allowed to pass the disk key to this content provider using this public key provided on the media possibly accompanied with a request to the host, either protected or not, identifying a decoder upon which play-back is desired. In receiving a legitimate disk key encrypted with the content provider's public key, the content provider may have a high level of confidence in this being a legitimate disk and, therefore, may send back an authorized public key for the particular decoder, or a list of authorized public keys, encrypted with the private key corresponding to the content provider's public key found on the media. The media device is then able to decrypt that list with this key.

Since, in Sims, media device decrypts that list with this key, Sims is not "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," as recited in claim 1.

Sims neither teaches, discloses, nor suggests "deriving the license information outside said secure area of the recording medium," as recited in claim 1. In Sims, rather, the encrypted disk key is provided to the play-back device decoder at step 313 to allow meaningful use of the content recorded thereon, not stored, as discussed above. There is thus no "license information outside said secure area of the recording medium" in Sims to derive. Claim 1 is submitted to be allowable. Withdrawal of the rejection of claim 1 is earnestly solicited.

Claims 6, 11, and 27 depend from claim 1 and add further distinguishing elements. Claims 6, 11, and 27 are thus also submitted to be allowable. Withdrawal of the rejection of claims 6, 11, and 27 is also earnestly solicited.

<u>Claims 18 and 28:</u>

The third clause of claim 18 recites:

Deriving said encrypted license information outside said secure area.

Sims neither teaches, discloses, nor suggests, "deriving said encrypted license information outside said secure area," as discussed above with respect to the rejection of claim 1.

The third clause of claim 18 recites further:

Storing the encrypted license information in the user-use area of the recording

medium or another recording medium.

Sims neither teaches, discloses, nor suggests, "storing the encrypted license information in the user-use area of the recording medium or another recording medium," as discussed above with respect to the rejection of claim 1. Claim 18 is thus submitted to be allowable as well, for at least those reasons discussed above with respect to the rejection of claim 1. Withdrawal of the rejection of claim 18 is earnestly solicited.

Claim 28 depends from claim 18 and adds further distinguishing elements. Claim 28 is thus also submitted to be allowable. Withdrawal of the rejection of claim 28 is also earnestly solicited.

Claims 1, 18, 27, and 28:

Claims 1, 18, 27, and 28 were rejected under 35 U.S.C. § 102(e) as anticipated by Sims. The rejection is traversed to the extent it would apply to the claims as amended. Reconsideration is earnestly solicited. Sims neither teaches, discloses, nor suggests, "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," or "deriving the license information outside said secure area of the recording medium," as discussed above with respect to the rejection of claim 1. Claim 1 is thus submitted to be allowable as well, for at least those reasons discussed above with respect to the rejection of claim 1. Withdrawal of the rejection of claim 1 is earnestly solicited.

Claim 27 depends from claim 1 and adds further distinguishing elements. Claim 27 is thus also submitted to be allowable. Withdrawal of the rejection of claim 27 is also earnestly solicited.

Claims 18 and 28:

Sims neither teaches, discloses, nor suggests, "deriving said encrypted license information outside said secure area," or "storing the encrypted license information in the user-use area of the recording medium or another recording medium," as discussed above with respect to the rejection of claim 1. Claim 18 is thus submitted to be allowable as well, for at least those reasons discussed above with respect to the rejection of claim 1. Withdrawal of the rejection of claim 18 is earnestly solicited.

Claim 28 depends from claim 18 and adds further distinguishing elements. Claim 28 is thus also submitted to be allowable. Withdrawal of the rejection of claim 28 is also earnestly

solicited.

Claim Rejections - 35 U.S.C. § 103:

Claim 15 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Nerlikar in view of U.S. Patent No. 5,191,611 to Lang. (hereinafter "Lang"). The rejection is traversed. Reconsideration is earnestly solicited.

Claim 15 depends from claim 1 and adds additional distinguishing elements. Nerlikar neither teaches, discloses, nor suggests "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," or "deriving the license information outside said secure area of the recording medium," as discussed above with respect to the rejection of claim 1. Lang shows no "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," or "deriving the license information outside said secure area of the recording medium," either, and thus cannot compensate for the deficiencies of Nerlikar with respect to claim 15. In Lang, rather, as described at column 2, lines 42-47,

> Additionally, a storage accessing device (used interchangeably herein with the following terms--personal accessing device (PAD) and smart card) provided with an encrypted or non-encrypted personal security key as well as personal identification code is included to allow an individual access to the storage medium or media.

Thus, a storage accessing device in Lang is provided with an encrypted or non-encrypted personal security key. No mention of "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," or "deriving the license information outside said secure area of the recording medium," as recited in claim 1, appears in Lang at all. Claim 15 is thus also submitted to be allowable. Withdrawal of the rejection of claim 15 is earnestly solicited.

Sims in view of Lang:

Claim 15 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Sims in view of Lang. The rejection is traversed. Reconsideration is earnestly solicited.

Claim 15 depends from claim 1 and adds additional distinguishing elements. Sims neither teaches, discloses, nor suggests, "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the

recording medium as the predetermined information," or "deriving the license information outside said secure area of the recording medium," as discussed above with respect to the rejection of claim 1. Lang shows no "storing license information based on use rights for using the encrypted electronic data stored in the user-use area to the secure area of the recording medium as the predetermined information," or "deriving the license information outside said secure area of the recording medium," either, and thus cannot compensate for the deficiencies of Sims with respect to claim 15. Claim 15 is thus also submitted to be allowable. Withdrawal of the rejection of claim 15 is earnestly solicited.

Allowable Subject Matter:

The Applicant acknowledges with appreciation the indication that claims 7, 12, 13, 19, 21, 24, and 25 contain allowable subject matter.

Conclusion:

Accordingly, in view of the reasons given above, it is submitted that all of claims 1, 5, 6, 7, and 9-28 are allowable over the cited references. Allowance of all claims 1, 5, 6, 7, and 9-28 and of this entire application is therefore respectfully requested.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 16 Feb 07

By: _____
Thomas E. McKiernan
Registration No. 37,889

1201 New York Avenue, NW, 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501